



An Extended Guide · No. 2077

Ransomware at a Small Office: Decisions Before, During & After

How preparation, calm choices, and a tested
backup turn a disaster into a bad week

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. Ransomware is the nightmare version of a break-in — and the single best protection is boring: a backup you keep offline and have actually tested, set up long before anything goes wrong.

Ransomware, and how a small office survives it

Ransomware is the attack that locks up all your files and demands money to unlock them. It can freeze a small business cold — no invoices, no records, no email. This guide walks through the decisions you make before, during, and after an attack, so it's survivable instead of fatal.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. In 30-plus years I've seen how much the outcome depends on choices made long before the attack ever lands. I'm a tech helper, not a lawyer — so I'll help you prepare and recover, and point you to the right professional for the legal calls.

Here's the honest truth up front: the business that survives ransomware well is almost always the one with a good, tested, **offline** backup. With it, you can tell the attacker no and rebuild. Without it, you're stuck making an awful choice under pressure. Most of this guide is really about making sure you're in the first group.

★ Let's get you ransomware-ready before you need it

The prep that beats ransomware — offline tested backups, MFA, updates — is exactly the hands-on work I do. In a visit or two I can get you set up so an attack is a bad week, not the end of your business. Call or text me at (330) 200-8042.

The whole guide, on one page

If you remember only these things, you'll handle ransomware far better than most small offices.

- ❑ **Before:** keep **offline or immutable, tested** backups. This is the one thing that beats ransomware.
- ❑ **Before:** MFA everywhere, current updates, and careful email habits stop most attacks from landing at all.
- ❑ **During:** isolate affected machines from the network, leave them on, and call your **insurer's hotline first**.
- ❑ **During:** **don't rush to pay** — payment doesn't guarantee recovery and may carry legal and sanctions risk.
- ❑ **During:** involve **law enforcement** (FBI IC3) and use free help at **StopRansomware.gov**.
- ❑ **After:** restore from clean backups, rebuild carefully, and learn how they got in so it can't happen again.

! Paying is a last resort, not a first move

Paying the ransom feels like the fast way out, but it's a gamble — you may not get a working key, you may be marked as an easy target, and it can be legally risky. Never decide to pay alone or in a panic; involve your insurer, law enforcement, and a lawyer first.

What ransomware actually does

A quick, plain explanation so the rest of the guide makes sense.

Ransomware is malicious software that **scrambles (encrypts) your files** so you can't open them, then demands a payment — usually in cryptocurrency — for the key to unscramble them. One infected computer can spread it across your whole network, locking up shared drives, your accounting, customer records, everything.

Many modern attacks add a nastier twist: before locking your files, the crooks **copy** them and threaten to publish or sell your data unless you pay. So even a perfect backup doesn't make the threat disappear — which is one more reason prevention matters so much, and one more reason to involve the professionals who've seen it all.

It gets in the same ordinary ways most attacks do: a stolen or guessed password, a convincing email that got someone to click, or an unpatched machine left exposed. That's good news, really — it means the same basic defenses that stop everyday break-ins stop ransomware too.

✓ It's a crime, and you're the victim

Falling for ransomware doesn't make you careless or foolish — these crews are organized and convincing. The point of preparing isn't to feel blame; it's to make sure that if they come for you, they leave empty-handed.

Before, step one: the backup that beats ransomware

If you do nothing else from this guide, do this. A good backup is the difference between 'no thanks' and a ransom payment.

The reason a backup is so powerful against ransomware is simple: if you have clean copies of your files, you don't need the attacker's key. You can wipe the infected systems and restore. The crook's whole leverage — 'pay or lose everything' — disappears.

But there's a catch the attackers count on. If your backup is always connected — a drive plugged in, a sync folder open — the ransomware encrypts the backup too. That's why the backup has to be **offline or immutable**: disconnected when not in use, or stored so it can't be changed or deleted even by someone with your passwords.

! Untested backups fail exactly when you need them

A backup you've never restored from may be silently broken — wrong files, missing data, won't load. The only way to know it works is to **test a restore** before disaster, not during it. Our backup fire-drill guide walks you through a simple quarterly test.

The 3-2-1 idea, in plain English

There's a simple rule of thumb that makes your backups ransomware-resistant without any jargon.

- **3 copies** of your important data — the working copy plus two backups.
- **2 different places or kinds** of storage — not both on the same computer.
- **1 kept offline or offsite** — disconnected or in the cloud, out of the ransomware's reach.

For a small office that can be as humble as: your files on the work computer, a backup to a cloud service, and a backup to an external drive you plug in weekly and then unplug and put away. The unplugged drive is your safety net — ransomware can't encrypt a drive that isn't connected.

✓ Immutable cloud backups are the modern safety net

Many backup services now offer 'immutable' or 'versioned' storage that can't be altered or deleted for a set time — even by someone who steals your password. For a busy office that can't remember to swap a drive, that's a great fit. I can help you pick and set one up.

Before, step two: stop it from landing

Backups are your safety net, but the best outcome is the attack that never gets in. These are the controls that shut the usual doors.

- **MFA everywhere** — most ransomware starts with a stolen password; a second sign-in step stops it cold.
- **Current updates** — unpatched machines are a favorite way in; replace end-of-support software.
- **Careful email habits** — a convincing attachment or link is the classic entry; slow down before clicking.
- **Least privilege** — everyday accounts separate from admin, so one hijacked login can't lock everything.
- **Endpoint protection** — keep Microsoft Defender or your security tool on and updated on every machine.

None of this is exotic, and it's the same advice in nearly all our guides for a reason: these few habits stop the large majority of attacks. Our Microsoft 365, Google Workspace, and backup fire-drill guides walk through each one.

Before, step three: write the plan while it's calm

Decide how you'll respond before you're panicking. A plan on paper turns a crisis into a checklist.

Your ransomware plan doesn't need to be long. It needs to answer, in advance, the questions you won't want to figure out at 2 a.m.: Who do we call first? Where are our backups and how do we reach them? Who can approve big decisions? How do we keep running — invoicing, serving customers — while systems are down?

Keep a printed copy somewhere that doesn't depend on your computers, and make sure more than one person knows where it is and what's in it. Our guide 'The First Hour After a Hack' is essentially this plan's opening steps, and pairs perfectly with this one.

★ I'll help you build the plan in one sitting

We can write your one-page ransomware plan together — who to call, where the backups live, how to keep the doors open — in a single visit. Then it's ready if you ever need it. Call (330) 200-8042.

During: the first moves when you're hit

The screen shows a ransom demand. Here's what to do in the first minutes — and it echoes our first-hour guide for good reason.

- ❑ **Stay calm** — the damage is done; careful beats fast now.
- ❑ **Isolate** affected machines from the network — unplug the cable or turn off Wi-Fi — but leave them ON.
- ❑ **Don't power off or wipe** — forensics and your insurer may need the machine's state.
- ❑ **Photograph the ransom note** and start a dated log of what you see and do.
- ❑ **Call your cyber-insurer's hotline first** — they bring in the experts and run the response.
- ❑ **Don't pay or reply** to the attackers yet — that's a decision for later, with professional advice.

! Isolate fast to stop the spread

Ransomware races to encrypt as much as it can reach, so disconnecting affected machines from the network quickly can save the computers it hasn't reached yet. Pull them off the network — but don't shut them down.

What ransomware readiness looks like for you

The before-during-after is the same for everyone, but a solo shop and a public office face different stakes and, in one case, a special legal rule.

If you're a small private business

Your focus is simple and powerful: good offline tested backups, strong prevention, and cyber insurance so a response team is a phone call away. With those, you can usually recover without ever paying.

- Set up offline or immutable backups and test a restore quarterly.
- Turn on MFA everywhere and keep updates current.
- Carry cyber insurance and know your incident hotline number.
- If hit, isolate, call the insurer first, and don't rush to pay.

If you're a township, village, or public body

You have everything above plus a special Ohio rule: a public body generally cannot pay a ransom unless its legislative authority formally votes to approve it — and there are tight incident-reporting deadlines.

- Build the same backups and prevention — lean on free CISA and CyberOhio help.
- Remember the ransom decision requires a formal board vote by resolution or ordinance.
- Report incidents on Ohio's clocks — 7 days to Homeland Security, 30 days to the Auditor of State.
- See our public-body cybersecurity guide for the full set of rules.

★ Private shop or public office, I can get you ready

The prevention and backup work is the same either way, and I handle the hands-on side for both. For public bodies I'll help you line it up with the legal rules your counsel confirms. Call (330) 200-8042.

During: the decision about paying

This is the hardest moment, and the one most likely to be made wrong under pressure. Let's think it through calmly, in advance.

The attacker wants you scared and rushed, often with a ticking countdown. Don't let that clock drive you. Paying the ransom is genuinely a **last resort**, and here's why: there's no guarantee you'll get a working decryption key, paying marks you as a business that pays (inviting the next attack), and the money funds more crime.

There can also be real **legal and sanctions risk** — paying certain groups can itself break the law. This is exactly why the decision must involve your insurer, law enforcement, and a lawyer. It is not a call to make alone, and never one to make in the first panicked hour.

! A good backup makes this decision easy

The whole reason we hammer on offline tested backups is this moment. With a clean backup, 'should we pay?' often becomes 'no — we'll restore.' Prepare well before the attack and you may never have to face the hardest version of this choice.

During: who to bring in, and the free help

You are not meant to handle this alone. Here's the team and the free resources standing by.

- **Your cyber-insurer's incident team** — forensics and breach lawyers who run the response (call the hotline first).
- **A trusted IT professional** (like me) to help contain and plan recovery.
- **Law enforcement — the FBI's IC3 at ic3.gov** — to report the crime; fast reporting sometimes helps.
- **CISA's [StopRansomware.gov](https://stopransomware.gov)** — a free government resource with guidance and, for some strains, free decryption tools.
- **A lawyer** — for the legal and notification questions, and before any decision to pay.

Lean on them. For a small office, a cyber policy's response team is the difference between facing this alone and having experienced experts coordinating your recovery. Our cyber-insurance guides explain how to get that team in your corner before you ever need it.

During: keeping the business alive while you're down

Recovery takes time, so part of the plan is simply staying open while the systems are dark.

Think ahead about how you'd keep serving customers if your computers were locked for days. Could you take orders on paper? Reach customers through a phone or a personal device not on the affected network? Do you have printed copies of today's critical information — schedules, contacts, appointments?

This is also where cyber insurance can help beyond the technical fix: many policies cover **business interruption** — some of the income you lose while you're down. Knowing that's there takes a little of the financial terror out of the situation. Our coverage guide explains what a policy pays for.

✓ A little paper is a great backup plan

Even in a cloud world, a printed list of your key customers, vendors, and today's commitments — kept somewhere offline — can keep you functioning for the days your systems are being rebuilt. Low-tech, high-value.

After: restoring the right way

Once the experts give the go-ahead, recovery begins. Done carefully, it's done once; rushed, it can undo itself.

The safe path is to make sure the attacker is truly out, then rebuild clean: wipe or replace the infected machines and restore your files from a backup you've confirmed is clean. Restoring onto a system that's still compromised, or from a backup the ransomware already touched, just starts the nightmare over — so let the forensics team confirm the all-clear.

Change all your passwords from clean devices as part of this, turn MFA on everywhere if it wasn't already, and watch closely for signs the attacker tries to return. Patience here pays: a methodical rebuild is what makes the recovery stick.

! Don't restore until you're told the coast is clear

Restoring too early is a classic way to reinfect yourself — the malware's still lurking, waiting for your clean files to come back. Wait for the forensics confirmation and follow the order the experts give you.

After: the duties you may not realize you have

Getting your files back isn't always the end. If data was exposed, the law may require you to tell people.

Remember that many ransomware attacks copy your data before locking it. If that data included customers' personal information, you may have legal duties to notify them — under Ohio's breach-notification law and possibly others. That's a legal judgment, made with your lawyer and your insurer's breach counsel, based on what the forensics found.

This is one more reason not to wipe and 'move on' the instant your files are back. You need the evidence of what the attacker reached to answer the notification question honestly. Our Ohio breach-notification guide explains the 45-day clock and who must be told.

! A quick, important note

This guide explains the idea in plain English so you know what to ask about — it is general information, not legal or insurance advice, and it is not a substitute for reading the actual rule or policy. Laws and requirements change, and your situation may be different, so please confirm the current requirement with a lawyer, your insurance agent, or the agency itself before you rely on it.

After: learning so it can't happen again

The one good thing to salvage from an attack is the lesson. Close the door they came through, and the ones like it.

The forensics findings will usually tell you how they got in — a stolen password, a clicked attachment, an unpatched machine. Use that as a to-do list, not a source of blame. Then step back and shore up the whole picture, because where there's one gap there are often others.

- ❑ MFA on **every** account — the single biggest prevention win.
- ❑ Backups confirmed **offline/immutable and tested**.
- ❑ Updates current, end-of-support software replaced.
- ❑ Staff refreshed on spotting scam emails.
- ❑ Access reviewed — unused logins and admin rights removed.
- ❑ Cyber insurance in place (or reviewed) for next time.

A business that recovers and hardens is far safer than it was before the attack. Painful as it is, many owners come out the other side with the security they always meant to set up.

A special note for public bodies

If you serve a township, village, county office, or similar public body, Ohio adds rules that change how you handle ransomware.

Under Ohio's political-subdivision cybersecurity law, a public body generally **cannot pay a ransom** unless its legislative authority formally approves it — by resolution or ordinance stating why payment is in the public's best interest. No single official can quietly decide to pay. That vote has to be built into your incident plan ahead of time.

There are also tight reporting clocks after any incident: report to Ohio Homeland Security within 7 days and the Ohio Auditor of State within 30 days of discovery. Our public-body cybersecurity guide covers all of this in detail — if you're a local office, read it alongside this one.

✓ Bake the vote and the clocks into your plan

For a public office, your ransomware plan must include the ransom-approval vote and the two reporting deadlines up front. Deciding how you'll handle them calmly now beats scrambling to interpret the law during an attack.

Ransomware myths that get offices in trouble

A few comfortable beliefs are exactly what the attackers count on. Let's clear them up.

- **'We're too small to be a target.'** Small offices are favorites — weaker defenses, and the attacks are automated and indiscriminate.
- **'Paying is the quick fix.'** Payment doesn't guarantee a working key, invites repeat attacks, and can be illegal.
- **'Our antivirus will stop it.'** Helpful, but no tool replaces MFA, updates, and offline tested backups.
- **'We back up, so we're fine.'** Only if the backup is offline and you've tested a restore — an always-connected backup gets encrypted too.
- **'If it happens, we'll figure it out then.'** The decisions are far better made calmly, in advance.

! The 'too small to matter' myth is the most expensive one

Attackers don't hand-pick small businesses — they cast a huge automated net and hit whoever has an open door. Being small doesn't make you invisible; it often just means fewer defenses. Prepare as if it could be you, because it can.

Why prevention is the cheap option

Set emotion aside and just look at the math — it makes the case for preparing all by itself.

An attack costs you far more than any ransom figure. There's the downtime with no income, the cost of recovery and rebuilding, possible legal and notification expenses, lost customers, and the hit to your reputation. Against all that, the prevention — turning on MFA, keeping tested backups, staying updated — is remarkably cheap, and much of the know-how is free.

Cyber insurance fits here too: for a manageable premium, you get a response team and help with the costs that a single attack could otherwise pile on. Premiums vary widely, so get quotes and compare — our cyber-insurance guides walk through what to look for and how to apply honestly.

✓ Spend a little before, or a lot after

Nearly every owner who's been through ransomware says the same thing: they wish they'd spent the small amount on prevention beforehand. You get to make that choice right now, on a calm day.

Your ransomware readiness, on one page

Here's the before-during-after boiled down to something you can post and actually use.

- ❑ **Before:** offline/immutable tested backups; MFA everywhere; updates current; a written plan and an emergency card.
- ❑ **During, step 1:** isolate affected machines from the network — leave them on.
- ❑ **During, step 2:** photograph the note, start a log, call the insurer's hotline first.
- ❑ **During, step 3:** involve the FBI (ic3.gov) and StopRansomware.gov; don't pay on impulse.
- ❑ **After, step 1:** restore from clean backups only after the experts say the coast is clear.
- ❑ **After, step 2:** check for notification duties, then learn and harden so it can't recur.

Print it, keep it somewhere offline, and make sure your team knows where it is. Ransomware will never be a good day, but with this plan it's a survivable one.

Three things you can do this week

You don't have to transform everything at once. Start with the three moves that matter most.

First, sort out your backups. Make sure you have a copy that's offline or immutable, and actually test restoring a file or two. This single step does more against ransomware than anything else.

Second, turn on MFA everywhere — email, cloud, remote access, admin accounts. It stops the stolen-password attacks that start so much ransomware. **Third, write your one-page plan and emergency card** so, if it ever happens, you're reaching for a checklist instead of guessing.

★ I'll knock out all three with you

Backups sorted and tested, MFA on everywhere, and a plan on paper — that's a visit or two, and it's the best money a small office can spend on security. No upsell, just the work. Call (330) 200-8042.

Common Questions

The questions owners ask me most about ransomware, answered plainly.

Remember: general information, not legal advice.

Q: Should we just pay to get our files back quickly?

Paying is a last resort, never a first move. There's no guarantee of a working key, it marks you as a payer, and it can carry legal and sanctions risk. Decide only with your insurer, law enforcement, and a lawyer — and if you have a clean backup, you often won't need to.

Q: Isn't my regular backup enough?

Only if it's offline or immutable and you've tested a restore. A backup that's always connected gets encrypted right along with your files. Keep a copy disconnected or in immutable cloud storage, and prove it works before you need it.

Q: Are we really a target? We're tiny.

Yes. Most ransomware is spread by automated attacks that hit whoever has an open door, regardless of size. Small offices are often easier targets, not safer ones. Prepare as if it could be you.

Q: What's the very first thing to do if we're hit?

Stay calm, isolate the affected machines from the network (leave them on), photograph the ransom note, and call your cyber-insurer's hotline first. Don't power off, don't wipe, and don't reply to the attackers yet. See our first-hour guide.

Q: Is there free help?

Yes. The FBI's IC3 (ic3.gov) takes crime reports, and CISA's StopRansomware.gov offers guidance and, for some strains, free decryption tools. Ohio public bodies can also lean on CyberOhio and have special reporting and ransom-vote rules.

★ Hit by ransomware right now?

Isolate the machines from the network, don't turn them off, and call your insurer's hotline — then call me and I'll help you work the plan. On a calm day, let's get you ready so it never comes to this. (330) 200-8042.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made ransomware at your small office feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

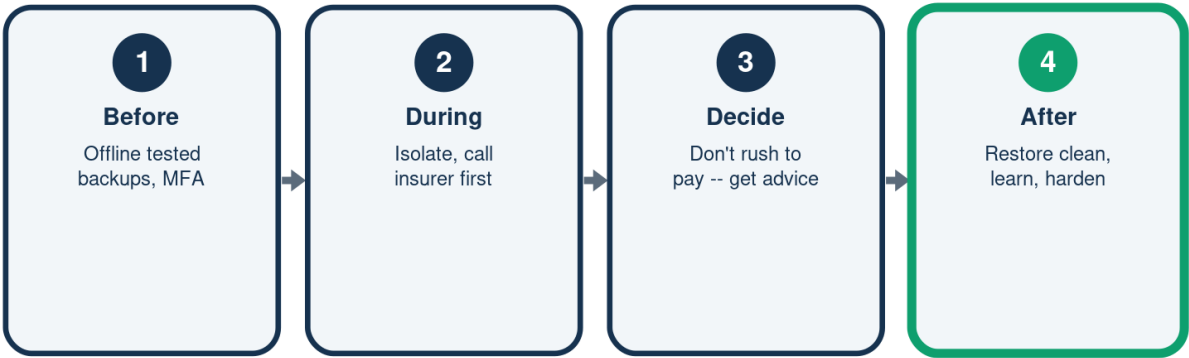
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

Before, During, After

Where the outcome is really decided



The business that prepares before is the one that survives after.

Why the Backup Type Matters

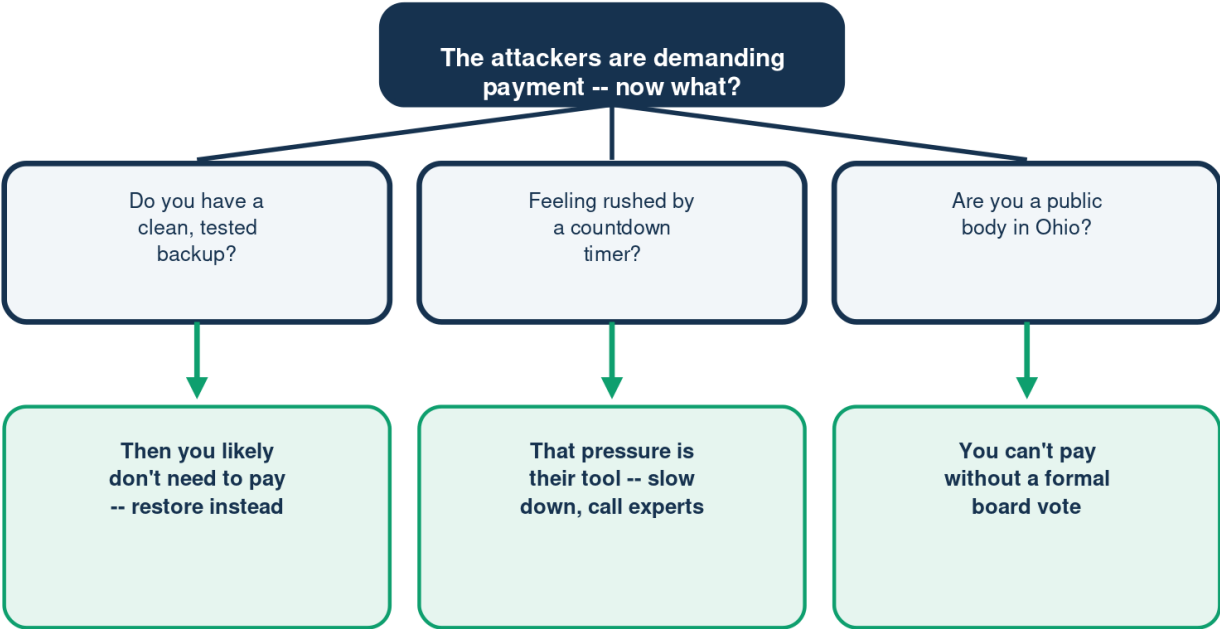
Ransomware encrypts whatever it can reach

	Backup kind	Survives ransomware?
Always connected	Encrypted too	No
Offline / unplugged	Out of reach	Yes
Immutable cloud	Can't be altered	Yes
Never tested	May not work	Unknown

Keep one copy offline or immutable -- and test a restore before you need it.

Should We Pay the Ransom?

A last resort, never a first move



Never decide alone -- involve your insurer, law enforcement, and a lawyer.

Illustration - a schematic, not to scale. Your setup may differ.

Prevention vs an Attack

The math makes the case

	Prevention	An attack
MFA + backups	Cheap, mostly free	n/a
Downtime	Minimal	Days with no income
Data loss	Restore and go	Maybe gone for good
Legal costs	Avoided	Notification, lawyers

Spend a little before, or a lot after -- you choose on a calm day.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech